REMARKS

The Office Action dated May 15, 2007, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1, 5, 7-13, 15-16, 19-21, and 24-25 have been amended to more particularly point out and distinctly claim the subject matter of the invention. New claims 26-28 have been added. No new matter has been added. Claims 1-25 are currently pending in the application and are respectfully submitted for consideration.

In the Office Action, at page 2, claims 1-25 were rejected under 35 U.S.C. 103(a) as being unpatentable over 3GPP TS 33.102 v5.1.0 (hereinafter '3GPP Security') in view of UMTS security. The Office Action took the position that 3GPP Security teaches all of the elements of the claim 1, with the exception of sending a request for registration. The Office Action then cited UMTS Security to cure the deficiencies of 3GPP Security. The rejection is respectfully traversed for the following reasons.

Independent claim 1, upon which claims 2-14 are dependent claims, recites a method in a communication system wherein a serving controller is configured to support a first security mechanism and at least one other security mechanism. The method includes sending a request for registration from a user equipment to a serving controller via a second controller. The request for registration includes information indicative of at least one security mechanism supported by the user equipment. The method also includes determining, based on the information, in the second controller that the user

equipment supports a second security mechanism other than a first security mechanism. The method further includes removing the information from the request for registration in the second controller, including in the request for registration an indication that the second security mechanism is used by the user equipment and forwarding the request for registration including said indication to the serving controller. The method additionally includes sending a challenge in accordance with the second security mechanism from the serving controller to the user equipment.

Independent claim 15, upon which claims 16-23 are dependent claims, recites a communication system. The system includes a serving controller configured to accept registrations of user equipments and to support at least two different security mechanisms. The system also includes a unit configured to receive from a user equipment in a request for registration data indicative of at least one security mechanism that the user equipment supports. The unit is further configured to remove said data from the request for registration, to provide the serving controller with information regarding a security mechanism supported by the user equipment that has requested to be registered to the serving controller. The unit is additionally configured to forward the request for registration to the serving controller, wherein the serving controller is configured to send a challenge in accordance with a determined security mechanisms to the user equipment and to authenticate a message from the user equipment based on a response to the challenge included in the message.

Claim 24 recites a proxy controller for a communication system, configured to receive a request for registration from a user equipment for forwarding to a serving controller, said request including data indicative of at least one security mechanism supported by said user equipment. The proxy controller for a communication system, further configured to determine based on said data a security mechanism supported by the user equipment that has requested to be registered to the serving controller, to remove the data from the request for registration in the second controller before forwarding said request to the serving controller, and to signal information to the serving controller regarding the security mechanism supported by the user equipment.

Claim 25 recites a communication system that includes first sending means for sending a request for registration from a user equipment to a serving controller via a second controller, said request including information indicative of at least one security mechanism supported by the user equipment. The system also includes determining means for determining, based on the information, in a second controller that the user equipment supports a second security mechanism other than a first security mechanism. The system further includes removing means for removing at said second controller said data. The system additionally includes second sending means for sending from the second controller to the serving controller an indication that the second security mechanism other than the first security mechanism is used by the user equipment. The system also includes third sending means for sending a challenge in accordance with the second security mechanism from the serving controller to the user equipment.

Independent claim 26 recites a communication system that includes serving controller means for accepting registrations of user equipments and to support at least two different security mechanisms. The system also includes means for receiving from a user equipment in a request for registration data indicative of at least one security mechanism that the user equipment supports, removing said data from the request for registration. The system further includes means for providing the serving controller with information regarding a security mechanism supported by the user equipment that has requested to be registered to the serving controller. The system additionally includes means for forwarding the request for registration to the serving controller, wherein the serving controller is configured to send a challenge in accordance with a determined security mechanism to the user equipment and to authenticate a message from the user equipment based on a response to the challenge included in the message.

Independent claim 27 recites a proxy controller for a communication system. The controller includes receiving means for receiving a request for registration from a user equipment for forwarding to a serving controller said request including data indicative of at least one security mechanism supported by said user equipment. The controller also includes determining means for determining, based on said data, a security mechanism supported by the user equipment that has requested to be registered to the serving controller. The controller further includes removing means for removing the data indicative from the request for registration in the second controller before forwarding said request to the serving controller. The controller additionally includes signalling means

for signalling information to the serving controller regarding the security mechanism supported by the user equipment.

Independent claim 28 recites a communication system that includes a first sending unit configured to send a request for registration from a user equipment to a serving controller via a second controller, said request including information indicative of at least one security mechanism supported by the user equipment. The system also includes a determining unit configured to determine, based on the information, in a second controller that the user equipment supports a second security mechanism other than a first security mechanism. The system further includes a removing unit configured to remove at said second controller said data. The system additionally includes a second sending unit configured to send from the second controller to the serving controller an indication that the second security mechanism other than the first security mechanism is used by the user equipment. The system also includes a third sending unit configured to send a challenge in accordance with the second security mechanism from the serving controller to the user equipment.

Certain embodiments of present invention provides that in the event that a user equipment does not support a first security mechanism, another security mechanism acceptable to both the user equipment and a serving controller can be efficiently established without need for a prior step of transferring of information on supported security mechanisms.

As will be discussed below, the cited prior art fails to disclose or suggest all of the elements of the claims, and therefore fails to provide the advantages and features discussed above.

3GPP Security generally describes a security architecture, such as security features and security mechanisms, for the third generation mobile telecommunication system. As shown in Figure 14 of 3GPP Security, the MS (Mobile Station) sends the Initial L3 message (Location update request, CM service request, Routing area update request, attach request, paging response etc.) to the VLR/SGSN. This message contains, for example, the user identity and the KSI. The included KSI (Key Set Identifier) is the KSI allocated by the CS service domain or PS service domain at the last authentication for this CN domain. See page 29 of 3GPP Security.

UMTS Security generally describes a security features that includes the first releases of the UMTS standards. UMTS also generally describes ciphering in the access network, and security protection of UMTS. See page 193 of UMTS Security.

In particular, the combination of 3GPP Security and UMTS Security teaches a prior step of a mobile subscriber (MS) transferring UE security capability to a serving radio network controller (SRNC) during RRC connection establishment and the SRNC storing the UE security capability. Then, during the set up procedure, in response to an "Initial L3 message" sent by the MS, a VLR/SGSN determines a list of allowed UMTS encryption and integrity algorithms (UEA, UIA) and sends these algorithms to the SRNC. The SRNC then determines which algorithms on the list are also supported by the MS,

and sends to the MS a message including the UIA and, if appropriate, the UEA. See 3GPP Security and UMTS Security.

Applicants respectfully submit that 3GPP Security fails to disclose or suggest all of the elements of the present claims. For example, 3GPP Security fails to disclose or suggest, at least, "sending a request for registration from a user equipment to a serving controller via a second controller, said request for registration including information indicative of at least one security mechanism supported by the user equipment," as recited in independent claim 1. As described above, 3GPP Security merely discloses a general procedure for ciphering and integrity protection. There is no teaching or suggestion of sending a request for registration from a user equipment to a serving controller via a second controller, said request for registration including information indicative of at least one security mechanism supported by the user equipment.

Applicants respectfully submit that UMTS Security does not cure the deficiencies of 3GPP Security. UMTS Security does not teach or suggest "sending a request for registration from a user equipment to a serving controller via a second controller, said request for registration including information indicative of at least one security mechanism supported by the user equipment," as recited in independent claim 1. Consequently, the combination of 3GPP Security and UMTS Security, whether viewed individually or combined, fails to teach or suggest all of the elements of independent claim 1.

Thus, for at least the reasons discussed above, Applicants respectfully assert that the combination of 3GPP Security and UMTS Security does not teach or suggest all of the elements of claim 1. Because claims 15, 24, and 25 recite similar features as in independent claim 1 (although they each have their own scope), the arguments as described above also apply to claims 15, 24, and 25. As such, Applicants respectfully request that the rejection of claims 1, 15, 24 and 25 be withdrawn.

For example, Applicants respectfully submit that the combination of 3GPP Security and UMTS Security fails to disclose or suggest, at least, "a unit configured to receive from a user equipment in a request for registration data indicative of at least one security mechanism that the user equipment supports, to remove said data from the request for registration, to provide the serving controller with information regarding a security mechanism supported by the user equipment," as recited in claim 15 and similarly recited in claims 24-25. Consequently, the combination of 3GPP Security and UMTS Security, whether viewed individually or combined, fails to teach or suggest all of the elements of independent claim 15 and similarly recited in claims 24-25. Applicants respectfully request that the rejection of claims 24 and 25 be withdrawn.

Claims 2-14 and 16-23 are dependent upon claims 1 and 15, respectively. Accordingly, claims 2-14 and 16-23 should be allowed for at least their dependencies upon claims 1 and 15, and for the specific limitations recited therein.

Applicants respectfully submit that the cited prior arts fail to disclose or suggest all of the elements of the claimed invention. These distinctions are more than sufficient

to render the claimed invention unobvious. It is therefore respectfully requested that all of claims 1-25 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Sejoon Ahn
Registration No. 58,959

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

SA:dc

Enclosures: Petition For Extension of Time (1 month)
Additional Claim Fee Transmittal
Check No. 17092